The Debrief

Key Takeaways on Data Privacy and Big Data from the National Association of Attorneys General Consumer Protection Conference

June 7, 2019

On May 20, 2019, Debevoise attended the public portion of the National Association of Attorneys General ("NAAG") Consumer Protection Spring Conference in Washington, D.C. The conference included several panels on key consumer-related issues facing state attorneys general, touching upon issues of consumer data privacy, robocalls and cryptocurrency regulation.

Debevoise & Plimpton

Below is a summary of two of the panels that may be of interest. We would be happy to discuss any of these topics further with our clients and friends.

- **Panel of Attorneys General** (Hawaii, Kansas, Maryland, North Carolina, South Carolina and South Dakota)

  - **Robocalls**: All attorneys general identified combatting robocalls as a top priority on their consumer-protection agendas. While there was general agreement about the volume of complaints agencies were receiving about robocalls, there was some recognition that this national problem likely required a national solution.

  - **State Data Breach Notification Laws**: The group discussed areas for development in consumer notification laws in each of their states. Notably, the North Carolina General Assembly has identity theft protection legislation currently pending that has the support of the State Attorney General's office.

  - **Proposed Federal Data Protection Legislation**: The attorneys general acknowledged the complexity businesses face when complying with all of the different state notification laws. While all the panelists recognized the utility of a national standard, there was also a general desire to preserve state jurisdiction and a concern about federal preemption. The South Dakota and North Carolina Attorneys General expressed their belief that states should maintain the ability to enforce both the proposed federal law and any relevant state laws regarding post-breach notification obligations.

- **Breaches of State and Local Systems**: States and municipalities are not immune to the growing threat of cyberattacks as both South Carolina and Maryland have experienced firsthand. South Carolina's Department of Revenue experienced a cyberattack in 2012, during which international hackers accessed a server containing approximately 3.6 million Social Security numbers. Similarly, the City of Baltimore recently experienced a ransomware attack that shut down some City systems for over three weeks. The Attorneys General recognized that there are significant hurdles both the public and private sector face to fully secure their systems against cyber threats.

- **Privacy and Big Data: The Short- and Long-Term Horizon**

  - A panel of current and former regulators, as well as law professors, spoke on how the "big data" landscape is affecting privacy regulation, and what might be done to effectively regulate data brokers.

  - **Regulatory Interest Coupled with Regulatory Uncertainty**: In general, while there is significant legislative and regulatory interest in consumer data privacy and data security law, the panelists doubted Congress' ability to make substantial progress on the issue in the near future. They noted, however, that state legislatures have been active in this space and that the California Consumer Protection Act is set to take effect in 2020 with other states like Washington poised to follow.

  - **Growth of the Plaintiffs' Bar**: As state legislatures begin to contemplate enacting legislation providing consumers with private rights of action for data breaches, the plaintiffs' bar will become more active in this area, especially when the California Consumer Protection Act takes effect at the beginning of 2020. The development of private rights of actions presents a trade-off for attorneys general. While these provisions empower consumers to protect their own privacy rights, they also mean that attorneys general may have to surrender control in shaping the direction of enforcement as courts begin to issue decisions on the scope of the law and companies' obligations.

  - **Regulation of Artificial Intelligence**: The panelists noted that there are serious oversight and enforcement challenges posed by machine-learning algorithms. Because "you can't interrogate an algorithm," there is no clear path to effective regulation and enforcement until there are advances in both the law and the technology available to regulators.

Courtney M. Dankworth
Partner, New York
+1 212 909 6758
cmdankworth@debevoise.com

Luke Dembosky
Partner, Washington D.C.
+1 202 383 8020
ldembosky@debevoise.com

Jeremy Feigelson
Partner, New York
+1 212 909 6230
jfeigelson@debevoise.com

Jim Pastore
Partner, New York
+1 212 909 6793
jpastore@debevoise.com

Christopher S. Ford
Associate, New York
+1 212 909 6881
csford@debevoise.com

Alexandra P. Swain
Associate, New York
+1 212 909 6792
apswain@debevoise.com